

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-268096
 (43)Date of publication of application : 29.09.2000

(51)Int.CI. G06F 17/60
 G06F 12/00
 G06F 12/14
 G06F 13/00
 H04L 12/54
 H04L 12/58
 H04N 7/167
 H04N 7/173
 // G06F 17/30

BEST AVAILABLE COPY

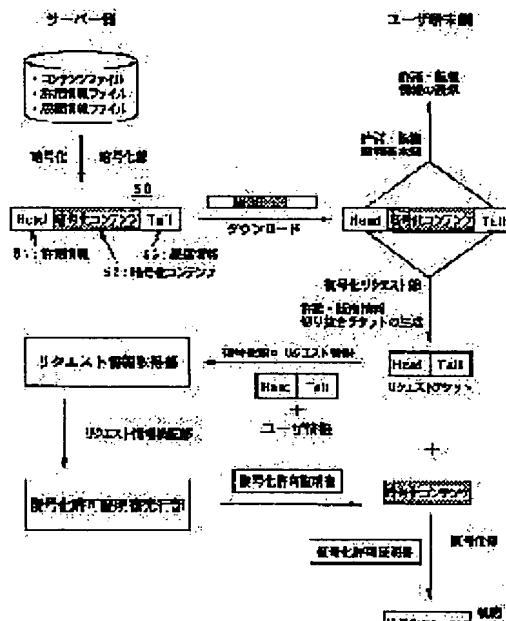
(21)Application number : 11-073011 (71)Applicant : DAINIPPON PRINTING CO LTD
 (22)Date of filing : 18.03.1999 (72)Inventor : MAKITA SHINICHI
 SAITO MASA
 WADA KEI

(54) CONTENTS DISTRIBUTION SYSTEM AND SERVER THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents distribution system with which permission/ copyright information is presented to a user before contents, the contents can be viewed on the condition of agreement from the user and the side of server can confirm and guarantee the complete distribution of contents from the side of server.

SOLUTION: The server prepares a contents file containing enciphered contents data and agreement information and transmits the contents file corresponding to contents designated to a distribution request from a user terminal to the user terminal. The user terminal finds the agreement of the user on contents by presenting the agreement information in the received contents file to the user. The user terminal sends a deciphering request containing the agreement information to the server. The server verifies the agreement information and when the verified result is normal, the permission of deciphering containing key information for deciphering the enciphered contents data is returned. The user deciphers the contents data and views the contents.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開2000-268096

(P2000-268096A)

(43)公開日 平成12年9月29日(2000.9.29)

(51) Int.Cl. 17/60 12/00 12/14 5 3 7 3 2 0

F I		テーマコード*(参考)	
G 0 6 F	15/21	3 3 0	5 B 0 1 7
	12/00	5 3 7 H	5 B 0 4 9
		5 3 7 M	5 B 0 7 5
	12/14	3 2 0 B	5 B 0 8 2
		3 2 0 F	5 B 0 8 9

審査請求 未請求 請求項の数15 O.L. (全 13 頁) 最終頁に続く

(21)出願番号 特願平11-73011

(22)出願日 平成11年3月18日(1999.3.18)

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 牧田 伸一

東京都新宿区市谷加賀町

大日本印

斎藤 雅

東京都新宿区市谷加賀

大日本印刷株式会社

(74) 代理人 100083839

弁理士 石川 泰男

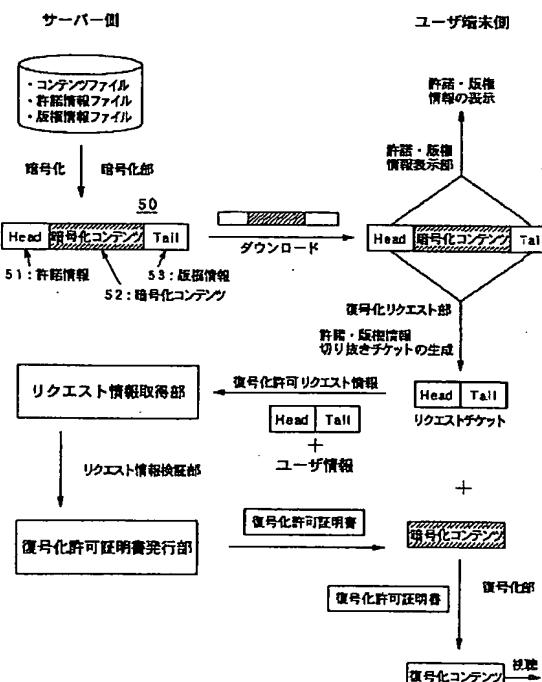
最終頁に統く

(54) [発明の名称] コンテンツ配信システム及びそのサーバ

(57) 【要約】 (修正有)

【課題】 ユーザに許諾・版権情報をコンテンツに先だって提示し、ユーザの同意を条件にコンテンツを視聴可能とすると共に、サーバ側からのコンテンツの配信が完全に行われたことをサーバ側で確認、保証することが可能なコンテンツ配信システムを提供する。

【解決手段】 サーバは、暗号化されたコンテンツデータと、同意情報を含むコンテンツファイルを作成し、ユーザ端末からの配信要求に対し指定されたコンテンツに対応するコンテンツファイルをユーザ端末へ送信する。ユーザ端末は、受け取ったコンテンツファイル中の同意情報をユーザに提示してその内容に対するユーザの同意を求める。ユーザ端末は同意情報を含む復号化要求をサーバへ送る。サーバは、同意情報を検証し、検証結果が正常であると、暗号化されたコンテンツデータを復号化するためのキー情報を含む復号許可を返信する。ユーザはコンテンツデータの暗号化を解除し、コンテンツを視聴する。



【特許請求の範囲】

【請求項1】 ネットワークを介して通信可能なサーバ及びユーザ端末を含むコンテンツ配信システムにおいて、

前記サーバは、

同意情報及び暗号化されたコンテンツデータを含み、前記同意情報が少なくとも末尾部に配置されたコンテンツファイルを作成する作成手段と、

ユーザ端末からのコンテンツ配信要求に応じて、指定されたコンテンツに対応するコンテンツファイルを送信する送信手段と、

ユーザからの復号化要求を受け取り、当該復号化要求に含まれる同意情報を検証する検証手段と、

検証結果が正常である場合に、前記暗号化されたコンテンツデータを復号化するためのキー情報を含む復号化許可を前記復号化要求元のユーザ端末へ送信する復号化許可部と、を備え、

前記ユーザ端末は、

希望するコンテンツの指定を含むコンテンツ配信要求を前記サーバへ送信する配信要求手段と、

前記サーバから受け取ったコンテンツファイル中の同意情報を取り出し、ユーザに提示して当該同意情報に対するユーザの同意を求める同意要求手段と、

前記同意情報に対するユーザの同意が得られた場合に、前記同意情報を含む復号化要求を作成して前記サーバへ送る復号化要求手段と、を備えるコンテンツ配信システム。

【請求項2】 前記サーバは、前記同意情報を含む検証用データを記憶する手段をさらに備え、前記検証手段は、ユーザ端末から送信された復号化要求に含まれる同意情報と前記検証用データに含まれる同意情報を照合し、両者が一致する場合に検証結果が正常であると判断する請求項1に記載のコンテンツ配信システム。

【請求項3】 前記サーバは、前記検証手段による検証結果が異常である場合に、前記送信手段により前記コンテンツファイルを再送信する請求項1又は2に記載のコンテンツ配信システム。

【請求項4】 前記復号化要求は、前記復号化要求を発するユーザのユーザ情報を含み、前記サーバは、前記復号化要求を記憶する記憶手段を備える請求項1乃至3のいずれかに記載のコンテンツ配信システム。

【請求項5】 前記ユーザ端末は、前記サーバから取得したキー情報を使用してコンテンツファイル中の暗号化されたコンテンツデータを復号化する復号化手段をさらに備える請求項1乃至4のいずれかに記載のコンテンツ配信システム。

【請求項6】 前記作成手段は、前記同意情報を前記コンテンツファイルの先頭部及び末尾部に分割して配置する請求項1乃至5のいずれかに記載のコンテンツ配信システム。

【請求項7】 前記同意情報は、前記コンテンツに関連する使用許諾情報及び版権情報を含む請求項1乃至6のいずれかに記載のコンテンツ配信システム。

【請求項8】 ネットワークを介してユーザ端末へコンテンツを配信するコンテンツ配信システムのサーバにおいて、

同意情報及び暗号化されたコンテンツデータを含み、前記同意情報が少なくとも末尾部に配置されたコンテンツファイルを作成する作成手段と、

ユーザ端末からのコンテンツ配信要求に応じて、指定されたコンテンツに対応するコンテンツファイルを送信する送信手段と、

ユーザ端末から送信されると共に前記同意情報を含む復号化要求を受け取り、当該復号化要求に含まれる同意情報を検証する検証手段と、

検証結果が正常である場合に、前記暗号化されたコンテンツデータを復号化するためのキー情報を含む復号化許可を前記復号化要求元のユーザ端末へ送信する復号化許可部と、を備えるサーバ。

【請求項9】 前記同意情報を含む検証用データを記憶する手段を備え、前記検証手段は、ユーザ端末から送信された復号化要求に含まれる同意情報と前記検証用データに含まれる同意情報を照合し、両者が一致する場合に検証結果が正常であると判断する請求項8に記載のサーバ。

【請求項10】 前記検証手段による検証結果が異常である場合に、前記送信手段により前記コンテンツファイルを再送信する請求項8又は9に記載のサーバ。

【請求項11】 前記復号化要求は、前記復号化要求を発するユーザのユーザ情報を含み、前記サーバは、前記復号化要求を記憶する記憶手段をさらに備える請求項8乃至10のいずれかに記載のサーバ。

【請求項12】 前記作成手段は、前記同意情報を前記コンテンツファイルの先頭部及び末尾部に分割して配置する請求項8乃至11のいずれかに記載のサーバ。

【請求項13】 前記同意情報は、前記コンテンツに関連する使用許諾情報及び版権情報を含む請求項8乃至12のいずれかに記載のサーバ。

【請求項14】 ネットワークを介して通信可能なサーバ及びユーザ端末を含むコンテンツ配信システムにおいて、

前記サーバは、

ユーザ端末からのコンテンツ配信要求に応じて、指定されたコンテンツに対応するコンテンツデータを送信する送信手段と、

前記ユーザ端末から受け取った受領情報を前記コンテンツデータと照合して、前記コンテンツデータがユーザ端末へ正常に送信されたことを確認する確認手段と、を備え、

前記ユーザ端末は、

希望するコンテンツの指定を含むコンテンツ配信要求を前記サーバへ送信する配信要求手段と、前記サーバから受け取ったコンテンツデータの先頭部及び末尾部を取り出し、受領情報としてサーバへ返送する手段と、を備えるコンテンツ配信システム。

【請求項15】 ネットワークを介してユーザ端末へコンテンツを配信するコンテンツ配信システムのサーバにおいて、

ユーザ端末からのコンテンツ配信要求に応じて、指定されたコンテンツに対応するコンテンツデータを送信する送信手段と、

ユーザ端末から送信され、前記サーバが送信したコンテンツデータの先頭部及び末尾部を含む受領情報をユーザ端末から受け取る手段と、

前記受領情報を前記コンテンツデータと照合して、前記コンテンツデータがユーザ端末へ正常に送信されたことを確認する確認手段と、を備えるサーバ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークなどの通信手段を介して情報を配信するシステムに関する。

【0002】

【従来の技術】従来、ネットワークなどの通信手段を介して、サーバ側からユーザ端末へ画像、音楽文章などの情報（以下、「コンテンツ」と呼ぶ。）を配信するサービスが行われている。このようなサービスは一般的に以下のようない手順で行われる。

【0003】まず、ユーザは自己の端末を操作してサービス元のサーバへ接続し、視聴したいコンテンツを決定し、そのコンテンツの配信をサーバへ要求する。サーバは、ユーザからの配信要求を受け取り、指定されたコンテンツのデータを要求元のサーバへ配信する。ユーザは、サーバから配信されたコンテンツのデータをダウンロードし、視聴する。

【0004】

【発明が解決しようとする課題】上記のような情報配信サービスにおける一つの問題に、コンテンツの内容に対する使用許諾・版権などをどのように扱うかということがある。配信されるコンテンツは、一般的に画像（動画、静止画を含む）、音楽、記事や小説などの文章などの著作物である場合が多い。このため、そのコンテンツに関する使用許諾や版権に関する情報（以下、「許諾・版権情報」と呼ぶ。）を視聴するユーザに提示し、同意を得る必要がある。従来のコンテンツ配信サービスでは、使用許諾や版権に対する同意を得る方法として、以下の2つの方法が考えられる。

【0005】第1の方法は、コンテンツの許諾・版権情報をコンテンツ自体とは別のデータファイルとし、コンテンツ自体のデータファイルに添付して配信するものである。しかし、この方法によると、ほとんどの場合ユー

ザは許諾・版権情報を見ることなく、コンテンツのみを視聴してしまう。従って、現実にはそのコンテンツの許諾・版権情報をユーザに提示することは難しい。また、ユーザがデータファイルを開いて許諾・版権情報を見た場合でも、ユーザがその内容に同意したか否をサーバ側で確認することはできない。

【0006】一方、第2の方法は、許諾・版権情報をコンテンツと一緒に暗号化して配信する方法である。このような場合には、コンテンツの配信後に、通常、暗号化を解除するための情報（例えば、暗号化のキー情報）をユーザに与えてユーザが視聴できるようにする処理が必要となるが、許諾・版権情報がコンテンツと一緒に暗号化されているので、暗号化を解除するキー情報を与えてしまうと、コンテンツを使用することが可能となってしまい、第1の方法と同じことになる。従って、いざれにしても、ユーザに許諾・版権情報のみをコンテンツに先だって提示し、ユーザの同意を条件にコンテンツを視聴可能にすることはできない。

【0007】また、このような配信サービスに関連する別の問題として、サーバ側から送信したコンテンツのデータがユーザ側で完全に受信できたかどうかをサーバ側が確認できないという問題がある。例えば、サーバ側からは全てのデータを送信した場合でも、ユーザ端末側若しくは通信経路中の何らかの事故、異常などに起因して、データ送信が途中で途切れてしまい、ユーザへ全てのデータを完全に配信できないことが生じうる。この場合、ユーザは要求したデータを完全に受け取ることはできず、しかもサーバ側はそのことを知ることができない。また、送信中に異常が生じたファイルを受け取り、それを開くことによりユーザ端末に何らかのトラブルが発生する危険性もある。

【0008】本発明は、以上の点に鑑みてなされたものであり、ユーザに許諾・版権情報をコンテンツに先だって提示し、ユーザの同意を条件にコンテンツを視聴可能とするコンテンツ配信システムを提供することを課題とする。

【0009】さらに、本発明は、サーバ側からのコンテンツの配信が完全に行われたことをサーバ側で確認、保証することが可能なコンテンツ配信システムを提供することを課題とする。

【0010】

【課題を解決するための手段】上記の課題を解決するため、請求項1記載の発明は、ネットワークを介して通信可能なサーバ及びユーザ端末を含むコンテンツ配信システムにおいて、前記サーバは、同意情報及び暗号化されたコンテンツデータを含み、前記同意情報が少なくとも末尾部に配置されたコンテンツファイルを作成する作成手段と、ユーザ端末からのコンテンツ配信要求に応じて、指定されたコンテンツに対応するコンテンツファイルを送信する送信手段と、ユーザからの復号化要求を受

け取り、当該復号化要求に含まれる同意情報を検証する検証手段と、検証結果が正常である場合に、前記暗号化されたコンテンツデータを復号化するためのキー情報を含む復号化許可を前記復号化要求元のユーザ端末へ送信する復号化許可部と、を備え、前記ユーザ端末は、希望するコンテンツの指定を含むコンテンツ配信要求を前記サーバへ送信する配信要求手段と、前記サーバから受け取ったコンテンツファイル中の同意情報を取り出し、ユーザに提示して当該同意情報に対するユーザの同意を求める同意要求手段と、前記同意情報に対するユーザの同意が得られた場合に、前記同意情報を含む復号化要求を作成して前記サーバへ送る復号化要求手段と、を備えるように構成する。

【0011】また、請求項8に記載の発明は、ネットワークを介してユーザ端末へコンテンツを配信するコンテンツ配信システムのサーバにおいて、同意情報及び暗号化されたコンテンツデータを含み、前記同意情報が少なくとも末尾部に配置されたコンテンツファイルを作成する作成手段と、ユーザ端末からのコンテンツ配信要求に応じて、指定されたコンテンツに対応するコンテンツファイルを送信する送信手段と、ユーザ端末から送信されると共に前記同意情報を含む復号化要求を受け取り、当該復号化要求に含まれる同意情報を検証する検証手段と、検証結果が正常である場合に、前記暗号化されたコンテンツデータを復号化するためのキー情報を含む復号化許可を前記復号化要求元のユーザ端末へ送信する復号化許可部と、を備えるように構成する。

【0012】上記のように構成されたコンテンツ配信システムによれば、サーバは、暗号化されたコンテンツデータを含み、同意情報が少なくともその末尾部に配置されたコンテンツファイルを作成する。ユーザ端末から配信要求がサーバへ送られると、サーバは指定されたコンテンツに対応するコンテンツファイルをユーザ端末へ送信する。ユーザ端末は、受け取ったコンテンツファイル中の同意情報を取り出し、ユーザに提示してその内容に対するユーザの同意を求める。ユーザが内容に同意すると、ユーザ端末は同意情報を含む復号化要求をサーバへ送る。サーバは、復号化要求中の同意情報を検証し、検証結果が正常であると、復号化許可をユーザ端末へ送る。この復号化許可は、先に送信したコンテンツファイル中の暗号化されたコンテンツデータを復号化するためのキー情報を含んでいる。従って、ユーザはこのキー情報を使用してコンテンツデータの暗号化を解除し、コンテンツを視聴することができる。

【0013】このように、サーバは同意情報に対するユーザの同意を条件に復号化許可をユーザに与えるので、ユーザが同意無しでコンテンツを視聴することが防止される。また、ユーザ端末からサーバへ送られる復号化要求は少なくともコンテンツファイルの末尾に配置された同意情報を含み、サーバはこの内容を検証するので、こ

の検証処理によりコンテンツデータのユーザ端末への配信が不完全であることが発見できる。よって、コンテンツのユーザ端末への配信保証を行うことができる。

【0014】請求項2に記載の発明は請求項1に記載のコンテンツ配信システムにおいて、前記サーバは、前記同意情報を含む検証用データを記憶する手段をさらに備え、前記検証手段は、ユーザ端末から送信された復号化要求に含まれる同意情報と前記検証用データに含まれる同意情報とを照合し、両者が一致する場合に検証結果が正常であると判断する。

【0015】また、請求項9の発明は、請求項8に記載のサーバにおいて、前記同意情報を含む検証用データを記憶する手段を備え、前記検証手段は、ユーザ端末から送信された復号化要求に含まれる同意情報と前記検証用データに含まれる同意情報とを照合し、両者が一致する場合に検証結果が正常であると判断する。

【0016】これらの発明によれば、同意情報の一致により、コンテンツファイルが確実に配信されたことをサーバ側で確認することができる。

【0017】請求項3に記載の発明は、請求項1又は2に記載のコンテンツ配信システムにおいて、前記サーバは、前記検証手段による検証結果が異常である場合に、前記送信手段により前記コンテンツファイルを再送信する。

【0018】また、請求項10に記載の発明は、請求項8又は9に記載のサーバにおいて、前記検証手段による検証結果が異常である場合に、前記送信手段により前記コンテンツファイルを再送信する。

【0019】これにより、コンテンツ配信が異常であった場合には、再度コンテンツの配信を行うことができる。

【0020】請求項4に記載の発明は、請求項1乃至3のいずれかに記載のコンテンツ配信システムにおいて、前記復号化要求は、前記復号化要求を発するユーザのユーザ情報を含み、前記サーバは、前記復号化要求を記憶する記憶手段を備える。

【0021】また、請求項11に記載の発明は、請求項8乃至10のいずれかに記載のサーバにおいて、前記復号化要求は、前記復号化要求を発するユーザのユーザ情報を含み、前記サーバは、前記復号化要求を記憶する記憶手段をさらに備える。

【0022】これにより、ユーザの同意に関する情報をサーバ側で記憶、管理しておくことが可能となる。

【0023】請求項5に記載の発明は、請求項1乃至4のいずれかに記載のコンテンツ配信システムにおいて、前記ユーザ端末は、前記サーバから取得したキー情報を使用してコンテンツファイル中の暗号化されたコンテンツデータを復号化する復号化手段をさらに備える。これにより、ユーザはコンテンツを自由に視聴できるようになる。

【0024】請求項6に記載の発明は、請求項1乃至5のいずれかに記載のコンテンツ配信システムにおいて、前記作成手段は、前記同意情報を前記コンテンツファイルの先頭部及び末尾部に分割して配置する。また、請求項12に記載の発明は、請求項8乃至11のいずれかに記載のサーバにおいて、前記作成手段は、前記同意情報を前記コンテンツファイルの先頭部及び末尾部に分割して配置する。これにより、コンテンツファイルの完全な配信をサーバ側で確実に確認することができる。

【0025】請求項7に記載の発明は、請求項1乃至6のいずれかに記載のコンテンツ配信システムにおいて、前記同意情報は、前記コンテンツに関連する使用許諾情報及び版権情報を含む。また、請求項13に記載の発明は、請求項8乃至12のいずれかに記載のサーバにおいて、前記同意情報は、前記コンテンツに関連する使用許諾情報及び版権情報を含む。これにより、ユーザーの使用許諾及び版権情報に対する同意を条件にコンテンツを提供することが可能となる。

【0026】請求項14に記載の発明は、ネットワークを介して通信可能なサーバ及びユーザ端末を含むコンテンツ配信システムにおいて、前記サーバは、ユーザ端末からのコンテンツ配信要求に応じて、指定されたコンテンツに対応するコンテンツデータを送信する送信手段と、前記ユーザ端末から受け取った受領情報を前記コンテンツデータと照合して、前記コンテンツデータがユーザ端末へ正常に送信されたことを確認する確認手段と、を備え、前記ユーザ端末は、希望するコンテンツの指定を含むコンテンツ配信要求を前記サーバへ送信する配信要求手段と、前記サーバから受け取ったコンテンツデータの先頭部及び末尾部を取り出し、受領情報としてサーバへ返送する手段と、を備える。

【0027】また、請求項15に記載の発明は、ネットワークを介してユーザ端末へコンテンツを配信するコンテンツ配信システムのサーバにおいて、ユーザ端末からのコンテンツ配信要求に応じて、指定されたコンテンツに対応するコンテンツデータを送信する送信手段と、ユーザ端末から送信され、前記サーバが送信したコンテンツデータの先頭部及び末尾部を含む受領情報をユーザ端末から受け取る手段と、前記受領情報を前記コンテンツデータと照合して、前記コンテンツデータがユーザ端末へ正常に送信されたことを確認する確認手段と、を備える。

【0028】上記の発明によれば、ユーザ端末は、サーバから受け取ったコンテンツデータの先頭部及び末尾部を受領情報として送信元のサーバへ返送する。サーバは、この受領情報を元のコンテンツデータと照合し、両者が一致すればコンテンツデータが正常にユーザへ配信されたことを確認できる。従って、コンテンツの配信保証を実現することができる。

【0029】

【発明の実施の形態】まず、本発明の基本的発想について図1を参照して概説する。本発明の好適な実施形態においては、ユーザにコンテンツを配信する際、コンテンツ自体のデータは暗号化し、これに暗号化していない許諾・版権情報を付加して送信する。具体的には、サーバはオリジナル（暗号化前）のコンテンツデータを暗号化して暗号化コンテンツ52を作成し、その前後に許諾情報51及び版権情報53を付加して暗号化コンテンツファイル52を作成し、記憶しておく。サーバ10は、ユーザからコンテンツの配信要求を受けると、そのコンテンツの暗号化コンテンツデータ50をユーザ端末へ送信する。

【0030】暗号化コンテンツデータ50をダウンロードしたユーザ端末は、まず許諾・版権情報をユーザに提示し、ユーザの同意を求める。ユーザがその内容に同意しない場合には、暗号化されたコンテンツを復号化するためのキー情報が与えられないため、ユーザはコンテンツを視聴することができない。一方、ユーザが許諾・版権情報の内容に同意すると、ユーザ端末は送信された暗号化コンテンツファイル50のヘッド部（先頭部）及びテール部（末尾部）のデータを組み合わせてリクエストチケットを作成し、これにユーザ情報を付加して復号化許可リクエスト情報を作成し、サーバへ送る。暗号化コンテンツファイルのヘッド部及びテール部にはそれぞれ許諾情報51及び版権情報53があるので、復号化許可リクエストは、許諾情報51及び版権情報53を含むファイルとなる。

【0031】サーバは、復号化許可リクエスト情報を受信して、ユーザが許諾・版権情報の内容に同意したことを知る。また、復号化許可リクエスト情報には、先にサーバが配信した暗号化コンテンツファイル50のヘッド部及びテール部が含まれているので、返送された復号化許可リクエスト情報中にこれらの部分が完全に含まれている場合には、コンテンツの配信が完全に行われたとみなすことができる。そして、以上の検証が正しく完了すると、ユーザ端末へ復号化のためのキー情報を含む復号化許可証明書を送る。ユーザ端末は、受信した復号化許可証明書中のキー情報を使用して暗号化コンテンツ52を復号化し、コンテンツを視聴することができる。

【0032】次に、本発明の好適な実施形態について詳細に説明する。

【0033】図2は、本発明の実施形態にかかるコンテンツ配信システムのブロック図である。図2において、コンテンツ配信システムは、ネットワーク1を介して通信可能なサーバ10及びユーザ端末30を備える。サーバ10は、ユーザが希望するコンテンツを配信する機能を有する。ユーザ端末30は、希望のコンテンツを指定してサーバからそのコンテンツの配信を受けるためにユーザが操作する端末装置により構成される。

【0034】サーバ10は、ネットワーク1との間のデ

ータ送受信を可能とするためのネットワーク接続部12を備える。また、サーバ10は、暗号化以前のコンテンツファイルを記憶するためのコンテンツファイルデータベース26、暗号化後の暗号化コンテンツファイルを記憶する暗号化ファイルデータベース28、ユーザからの復号化許可リクエストの検証に使用する検証用データを記憶するための検証用データベース24及び復号化許可リクエスト情報のログを記憶するためのログファイルデータベース22を備える。

【0035】さらに、サーバ10は、ユーザ端末からの配信要求に応答して暗号化コンテンツファイルを送信する配信要求処理部13と、ユーザ端末から送信される復号化許可リクエストを取得するリクエスト情報取得部14と、復号化許可リクエスト情報の内容を検証用データを用いて検証するリクエスト情報検証部16と、検証結果が正しい場合に復号化許可証明書を発行する復号化許可証明書発行部18と、を備える。なお、配信要求処理部13、リクエスト情報取得部14、リクエスト情報検証部16及び復号化許可証明書発行部18は、実際にはサーバ10上で実行されるプログラムとして実現することができる。

【0036】一方、ユーザ端末30は、ネットワーク1を介してサーバ10と通信するためのネットワーク接続部32を備える。また、ユーザ端末30は、サーバ10から送信された暗号化コンテンツファイル50を記憶するための暗号化ファイル記憶部40と、復号化後のコンテンツファイルを記憶するための復号化ファイル記憶部42と、を備える。

【0037】さらに、ユーザ端末30は、サーバ10から送信された暗号化コンテンツファイル50から許諾情報51及び版権情報53を取り出してユーザに提示する許諾・版権情報表示部36と、許諾情報及び版権情報を含む復号化許可リクエスト情報を作成及び送信する復号化リクエスト部34と、サーバ10からの復号化許可証明書に含まれる復号化キー情報を使用して暗号化コンテンツファイルを復号化するための復号化部38と、を備える。これら許諾・版権情報表示部36、復号化リクエスト部34及び復号化部38は、ユーザ端末上で実行されるプログラムにより実現することができる。特に、インターネットを利用した配信システムにおいては、これらの機能を閲覧ソフトウェア（いわゆるブラウザ）により実現することができる。

【0038】次に、図1乃至4を参照して、本発明のコンテンツ配信システムの動作について説明する。

【0039】まず、コンテンツ配信のための前処理として、サーバ10は各コンテンツについて暗号化コンテンツファイル50を作成し、暗号化ファイルデータベース28に記憶しておく。コンテンツファイルデータベース26は画像、音楽、文章などのコンテンツデータを暗号化していない状態で記憶している。また、コンテンツフ

ァイルデータベース26内には、各コンテンツに対応する許諾情報ファイル及び版権情報ファイルが各コンテンツと関連付けされて記憶されている。これは、例えば各コンテンツファイルにコンテンツ識別情報を割り当てて管理することにより実行される。

【0040】図4（A）及び（B）に許諾情報及び版権情報の例を示す。許諾情報は一般的に、著作物であるコンテンツの使用に関する制限条項を含み、版権情報はそのコンテンツの版権の所有者の情報などを含む。なお、これらの情報の具体的な内容は、各コンテンツの属性、種類、内容などに依存するが、いずれもその内容に対するユーザの同意を求める内容となっている。また、好ましくは、許諾情報及び版権情報は対応するコンテンツ識別情報を含んでいる。

【0041】暗号化部20は、コンテンツファイルデータベース26内に記憶されているコンテンツファイルを特定の暗号化方法により予め暗号化し、これに許諾情報及び版権情報を附加して暗号化コンテンツファイル50を作成する。暗号化コンテンツファイル50のデータ構造は図1に示されており、そのヘッド部（先頭部）に許諾情報51を有し、テール部（末尾部）に版権情報53を有し、その間に暗号化コンテンツ52が挟まれたデータ構造となっている。ここで、許諾情報51及び版権情報53は暗号化されておらず、通常は文章であるので例えばテキストデータのようなデータ形式とすることができる。暗号化部20は、こうして作成した暗号化コンテンツファイル50を暗号化ファイルデータベース28へ記憶する。暗号化ファイルデータベース28は、複数のコンテンツに対応する暗号化コンテンツファイル50を記憶している。

【0042】さらに、暗号化部20は、暗号化コンテンツファイル50の作成時に、そのコンテンツに対応する検証用データを作成する。検証用データとは、復号化許可リクエスト情報の検証処理において使用するデータであり、具体的にはそのコンテンツ識別情報、許諾情報51及び版権情報53などを含む。コンテンツファイルデータベース26内では各コンテンツに識別情報を割り当てて記憶しているので、その識別情報を検証用データに含めることができる。また、検証用データは、対応するコンテンツを暗号化した際のキー情報を含む。こうして作成された検証用データはコンテンツ識別情報によりコンテンツ毎に整理されて検証用データベース24へ記憶される。

【0043】以上の前処理が完了した状態で、コンテンツ配信処理が行われる。次に、コンテンツ配信処理を図1乃至3を参照して説明する。

【0044】まず、ユーザはユーザ端末30を操作してコンテンツ配信サービスを行うサーバ30へ接続し、配信を希望するコンテンツを決定し、配信要求を行う（ステップS1）。この配信要求は、ネットワーク接続部3

2、ネットワーク1、ネットワーク接続部12を介してサーバ30内の配信要求処理部13へ送られる。

【0045】配信要求処理部13は、配信要求において指定されたコンテンツに対応する暗号化コンテンツファイル50を暗号化ファイルデータベース28から取得し、ネットワーク接続部12を介してユーザ端末へ送信する(ステップS3)。

【0046】ユーザ端末30は、暗号化コンテンツファイル50を受け取り、暗号化ファイル記憶部40に記憶すると共に、図1に示すようにその先頭の許諾情報51と末尾の版権情報53を切り取って許諾・版権情報表示部36へ送る(ステップS5)。許諾・版権情報表示部36は、許諾情報51及び版権情報53をディスプレイなどの表示装置によりユーザに提示し、その内容に対する同意を求める(ステップS7)。許諾情報及び版権情報の表示例は図4に示されている。

【0047】ユーザが許諾情報51又は版権情報53の内容に同意しない場合には、処理は終了し、ユーザはコンテンツを視聴することはできない。

【0048】一方、ユーザが同意すると、許諾・版権情報表示部36は許諾情報51及び版権情報53を復号化リクエスト部34へ送る。復号化リクエスト部34は、図1に示すように許諾情報51及び版権情報53からリクエストチケットを作成し、これにその端末のユーザの情報(ユーザIDなど)を添付して復号化許可リクエスト情報を作成し、ネットワーク接続部32を介してサーバ10へ送信する(ステップS11)。

【0049】サーバ10は、リクエスト情報取得部14によりユーザ端末30から送信された復号化許可リクエスト情報を受け取り、それをログファイルデータベース22にログとして記憶する(ステップS13)。復号化許可リクエスト情報はユーザ情報を含んでいるので、これを記憶しておくことにより、当該ユーザがそのコンテンツの許諾・版権情報に同意した事實をサーバ側で記録しておくことが可能となる。また、リクエスト情報取得部14は、復号化許可リクエスト情報をリクエスト情報検証部16へ送る。

【0050】リクエスト情報検証部16は、受け取った復号化許可リクエスト情報のコンテンツに対応する検証用データを検証用データベース24から取得し、両者を照合する。即ち、リクエスト検証部16は、復号化許可リクエストに含まれる許諾情報51及び版権情報53を、検証用データ中の対応する情報と照合する(ステップS15)。両者が完全に一致する場合には、そのリクエストは正常なものであり、且つ、暗号化コンテンツファイルは正常にユーザ端末へ送信されたと判断し、復号化許可証明書発行部18へその旨を知らせる。同時に、検証用データベース24からそのコンテンツに対応する復号化キー情報を取得して、復号化許可証明書発行部18へ送る。

【0051】一方、ステップS15で検証結果が失敗した場合は、ユーザへ送信された暗号化コンテンツファイルが通信不良などの何らかの原因で完全に受信されなかつたとみなすことができる。実際に最も多く起こりうるのは、暗号化コンテンツファイルの送信が途中で途切れ、その末尾にあるはずの版権情報53が正しく受信されない場合である。この場合、復号化許可リクエスト情報中の版権情報と検証用データ中の版権情報は一致しないので、ステップS15の検証は失敗となる。従って、処理はステップS3へ戻り、暗号化コンテンツファイルの送信からやり直す。

【0052】ステップS15で検証が成功すると、復号化許可証明書発行部18は、復号化キー情報を含む復号化許可証明書を作成し、リクエスト元のユーザ端末へ送信する(ステップS17)。

【0053】ユーザ端末30では、復号化リクエスト部34が復号化許可証明書を受け取り、復号化部38へ送る。復号化部38は、先に暗号化ファイル記憶部40に記憶しておいた暗号化コンテンツファイル50から暗号化コンテンツ52を取得し、復号化許可証明書に含まれるキー情報を利用してコンテンツの復号化を行う(ステップS19)。そして、復号化されたコンテンツファイルを復号化ファイル記憶部42に記憶する。

【0054】こうして、コンテンツの暗号化が解除される。よって、ユーザは復号化ファイル42中のコンテンツデータを読み出して、視聴することができる。

【0055】なお、上記の実施形態においては、復号化許可リクエスト情報にユーザ情報を含め、サーバ側で復号化リクエスト情報のログを記録することにより、許諾・版権情報に同意したユーザの情報を管理するように構成している。これは、コンテンツの提供側としては、各ユーザの趣味、嗜好の傾向を探ることができる点で有益である。しかし、システムの設計上、そのような情報の管理が不要である場合には、復号化リクエスト中にユーザ情報を含める必要はなく、サーバ10におけるログの記録も省略することができる。

【0056】また、本発明のコンテンツ配信方法は有料であるか無料であるかを問わずに適用することができる。有料の配信サービスに適用する場合には、許諾・版権情報の代わりに、若しくはこれらに加えて、そのコンテンツ配信サービスの対価をユーザへ課金することに対するユーザの同意を求める情報を含め、ユーザに提示するように構成することができる。その場合、サーバ10はリクエスト情報検証処理において、当該ユーザの予納金の残高などを確認し、料金の徴収が可能な場合にのみ復号化許可証明書を発行するようすればよい。

【0057】また、提供すべきコンテンツに著作権などに基づく使用制限などが存在しない場合には、コンテンツの配信保証のみを目的としてシステムを構成することができる。その場合、コンテンツ自体を暗号化する必要

はなく、また、許諾・版権情報に相当する情報も特に存在しない。よって、コンテンツデータを暗号化せずに送信し、ユーザ端末は受信したコンテンツデータの先頭部及び末尾部の所定量のデータを受領情報（ユーザがコンテンツを受領したことを示す情報）としてサーバへ返送するように構成すればよい。サーバは、受信した受領情報最先に送信したコンテンツデータの先頭部及び末尾部と照合する。両者が一致すれば、そのコンテンツが正常にユーザへ配信されたことをユーザ側で確認することができる。

【0058】

【発明の効果】以上説明したように、本発明によれば、コンテンツ情報をのみを暗号化し、これに許諾・版権情報を添付してユーザに送信すると共に、許諾・版権情報に対する同意を条件にコンテンツ情報の復号化を許可するように構成したので、許諾・版権情報を無視してコンテンツ情報をのみを視聴することが防止できる。また、許諾・版権情報は暗号化されていないので、受信後速やかにユーザに提示することができる。

【0059】また、コンテンツファイルの少なくとも末尾部（好ましくは先頭部及び末尾部）に許諾情報及び版権情報を配置し、これらを復号化リクエストに含めてサーバへ送るので、コンテンツファイルの配信に異常が生じて完全な送信が完了していない場合は、その異常が復号化リクエスト情報中の許諾情報又は版権情報の異常として発見できる。さらに、配信の異常が発見された場合にはコンテンツの再配信を行うことができる。よって、復号化リクエストを受け取ることにより、配信側のサーバとしてはコンテンツの配信保証機能を確立する

ことができる。これは、例えば有料でコンテンツを配信するサービスを行う場合などにはサービスの信頼性を向上させる点で特に有効である。

【図面の簡単な説明】

【図1】本発明によるコンテンツ配信処理の概要を示す図である。

【図2】本発明の実施形態にかかるコンテンツ配信システムのブロック図である。

【図3】本発明によるコンテンツ配信処理を示すフローチャートである。

【図4】許諾情報及び版権情報の例を示す図である。

【符号の説明】

1…ネットワーク

10…サーバ

13…配信要求処理部

14…リクエスト情報取得部

16…リクエスト情報検証部

18…復号化許可証明発行部

20…暗号化部

22…ログファイルデータベース

24…検証用データベース

26…コンテンツファイルデータベース

28…暗号化ファイルデータベース

30…ユーザ端末

34…復号化リクエスト部

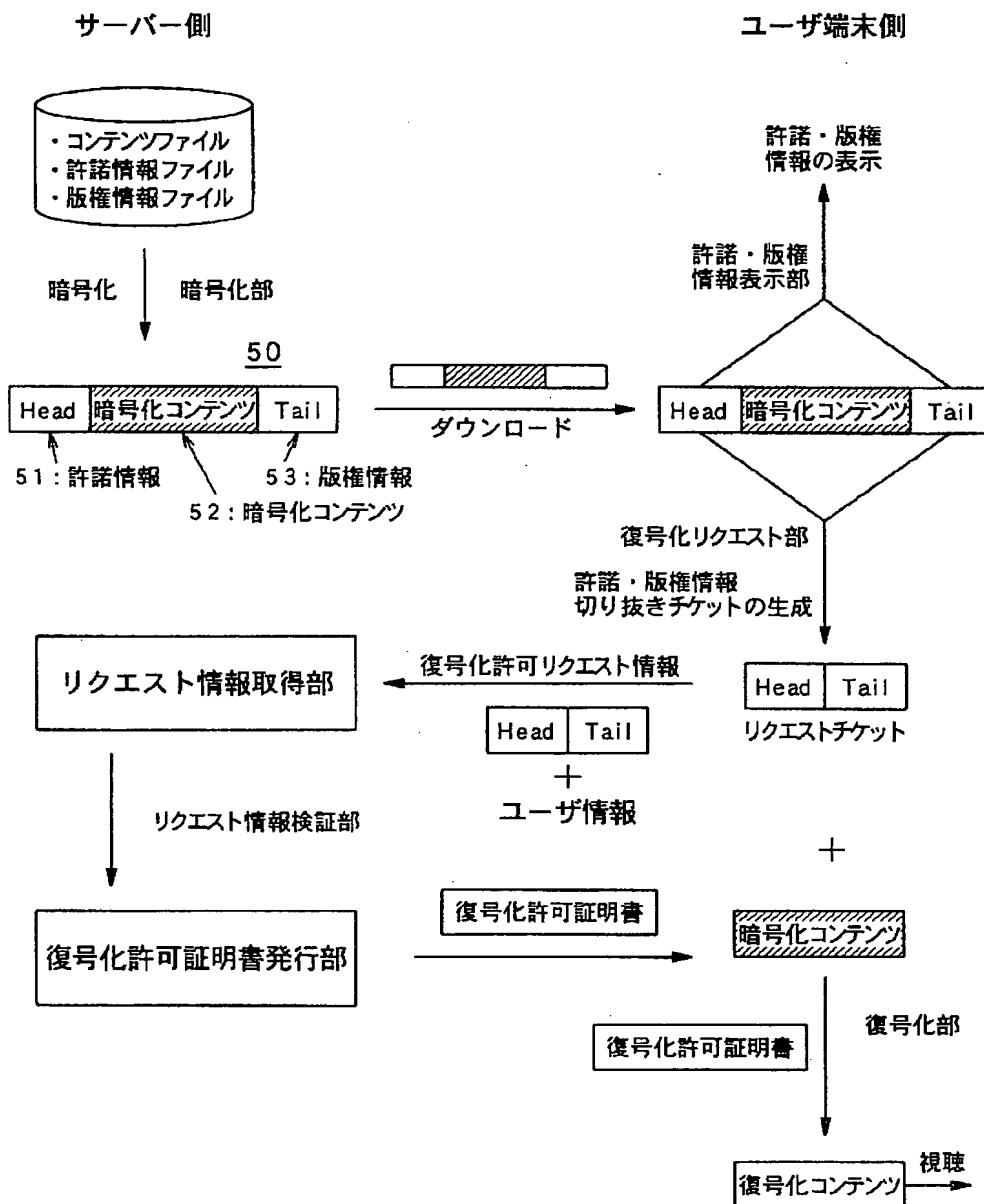
36…許諾・版権情報表示部

38…復号化部

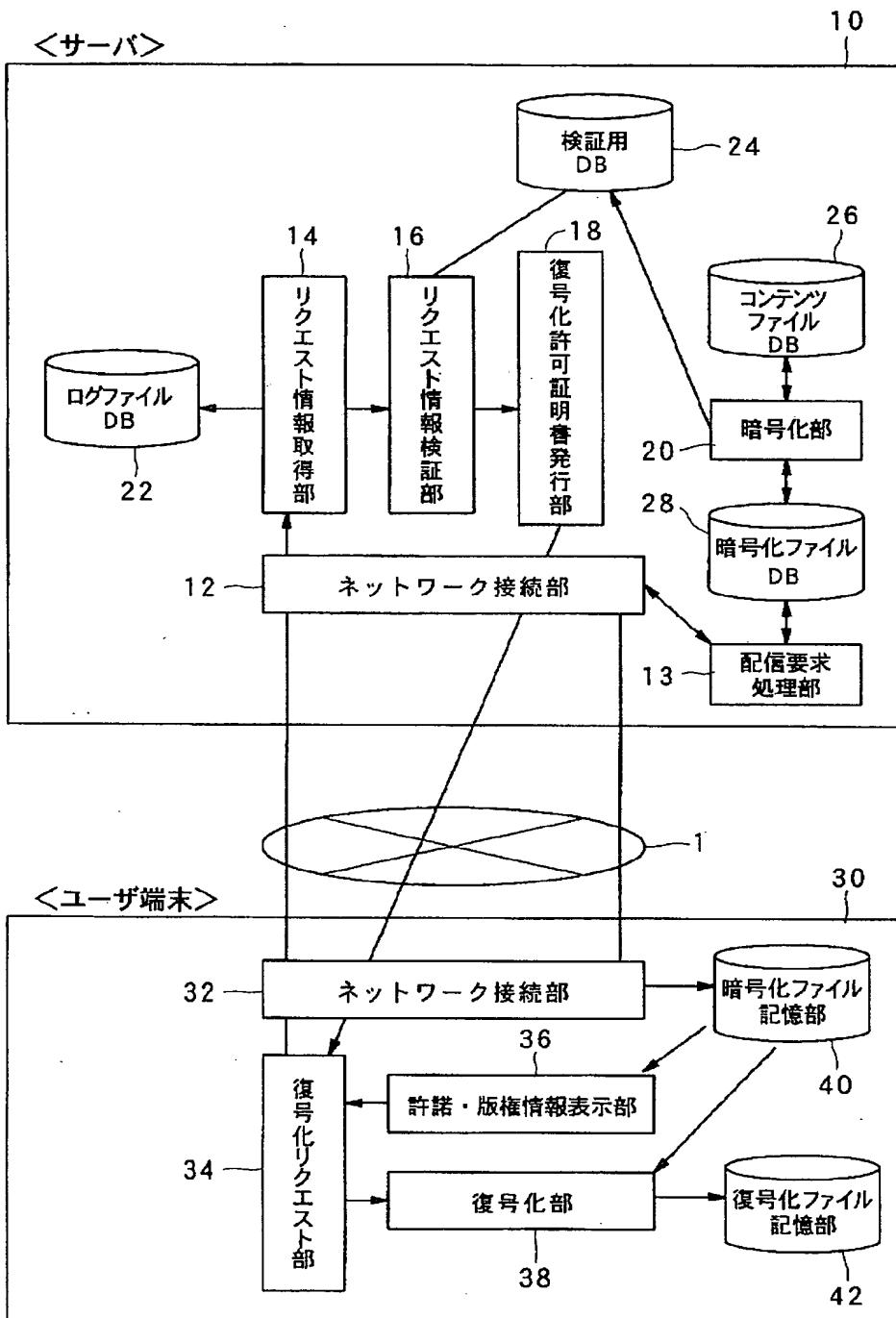
40…暗号化ファイル記憶部

42…復号化ファイル記憶部

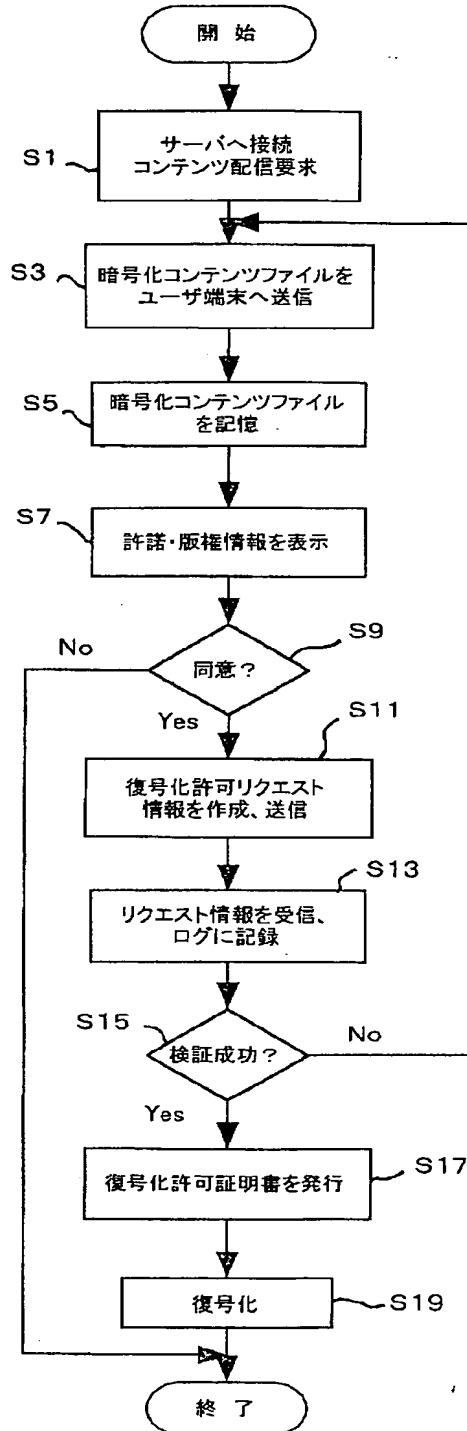
【図1】



【図2】



【図3】



【図4】

【許諾情報の例】

コンテンツNo. 0000 タイトル: △△△△ この作品の利用はあなたの個人的な楽しみに限り、営利目的の利用は禁止します。 また、非営利目的にあたっては印刷物としての配布は許可しますが、インターネットあるいはその他のあらゆる媒体を通じてデジタル形式で第三者に提供することを禁止します。但し、著作権者の許可を得た場合にはこの限りではありません。 あなたはこの内容に同意しますか？	<input type="button" value="同意する"/>	<input type="button" value="同意しない"/>
---	-------------------------------------	--------------------------------------

(A)

【版権情報の例】

コンテンツNo. 0000 タイトル: △△△△ この作品の著作権は以下の者に属します。 大日本太郎 大日本印刷株式会社 E-mail: ◇◇◇◇ Tel: XXX-XXXX 住所: □□□□ あなたはこの内容に同意しますか？	<input type="button" value="同意する"/>	<input type="button" value="同意しない"/>
---	-------------------------------------	--------------------------------------

(B)

フロントページの続き

(51) Int. Cl. 7	識別記号	F I	マーコード (参考)
G 06 F	13/00	3 5 4	G 06 F 13/00 3 5 4 D 5 C 06 4
H 04 L	12/54		H 04 N 7/173 5 K 03 0
	12/58		H 04 L 11/20 1 0 1 B
H 04 N	7/167		H 04 N 7/167 Z
	7/173		G 06 F 15/40 3 1 0 F
// G 06 F	17/30		3 2 0 B

(72)発明者 和田 圭

東京都新宿区市谷加賀町一丁目1番1号
大日本印刷株式会社内

F ターム(参考) 5B017 AA07 BA05 BA07 BB02 BB07
CA16
5B049 AA05 BB11 CC05 EE05 GG10
5B075 KK43 KK54 KK63 ND20 PQ05
5B082 AA11 AA13 EA01 EA07 EA12
GA02 GC03 GC05 HA08
5B089 GA11 GA21 GB01 JA32 JA33
JB01 JB16 JB22 JB24 KA12
KA17 KB06 KB13 KC57 KC58
KH30 LB14 ME08
5C064 BA07 BB02 BD02 BD03 BD08
BD09 BD14
5K030 GA15 HA06 KA01 KA07 LA02
LD12 LD19 LE12